Keep office information SECURE!

Blue Cross Blue Shield Blue Care Network of Michigan

NOVEMBER 2019

Tips to make your patients' information more secure

- **Notify Blue Cross Blue Shield of Michigan or Blue Care Network immediately** when a user no longer requires access to our system. (See Take the proper steps today on the right.)
- **Don't share user IDs.** Each employee who needs access should have an individual ID.
- **Protect passwords.** The safest passwords are hard-to-guess, never shared and never posted where others can see them. Create unique passwords that use a minimum of eight characters and have a combination of words, numbers, symbols and upper and lowercase letters.
- Use separate **Wi-Fi networks, one for your practice and another for personal devices or guest use (e.g., Practice, Practice Guest). Use separate passwords for each.**
- Make sure laptops and desktops are **secured** (cabled or stored in a locked drawer) when left unattended.
- **Lock your workstation screens** when not in use.
- Maintain a safe, confidential, and secure work area regardless of work location. Follow additional safeguards to protect PHI such as taking added precautions to prevent inadvertent disclosures such as storing PHI in locked cabinets or in a locked room.
- We strongly encourage you to **encrypt protected health information** stored on laptops to minimize the risk of a breach if a laptop is lost or stolen.
- **Require a user ID and password** at computer startup. We also recommend a user ID and password login after a designated period of inactivity.
- Diskettes, thumb drives and other removable media containing PHI should be **encrypted** before being removed from the facility.

Disable system access when employees depart

To safeguard protected health information and comply with federal law, health care providers must disable former employees' access to Blue Cross and BCN systems. Please disable employees' access when they leave their positions. If system access is not disabled and the former employee inappropriately accesses PHI, the **health care provider** is responsible for notifying affected members of the information breach, which could be very costly.

Take the proper steps today

It's easy to disable system access when an employee leaves or no longer requires access. Download and fax the Provider Secured Services ID Reassignment Form — to **1-800-495-0812**.

To access the document:

- Visit **bcbsm.com/providers**.
- Click *Modify Your Account*.
- Click *Deactivate ID* in the drop-down menu then the *Provider Secured Services ID Reassignment Form*.

If you have any questions, contact the Web Support Help Desk at **1-877-258-3932**. Hours of operation are Monday through Friday from 8 a.m. to 8 p.m.

Review access periodically

We recommend a review of your employees' access needs **every three months**. Large organizations might consider more frequent reviews depending on employee turnover or other operational concerns.

R091765